

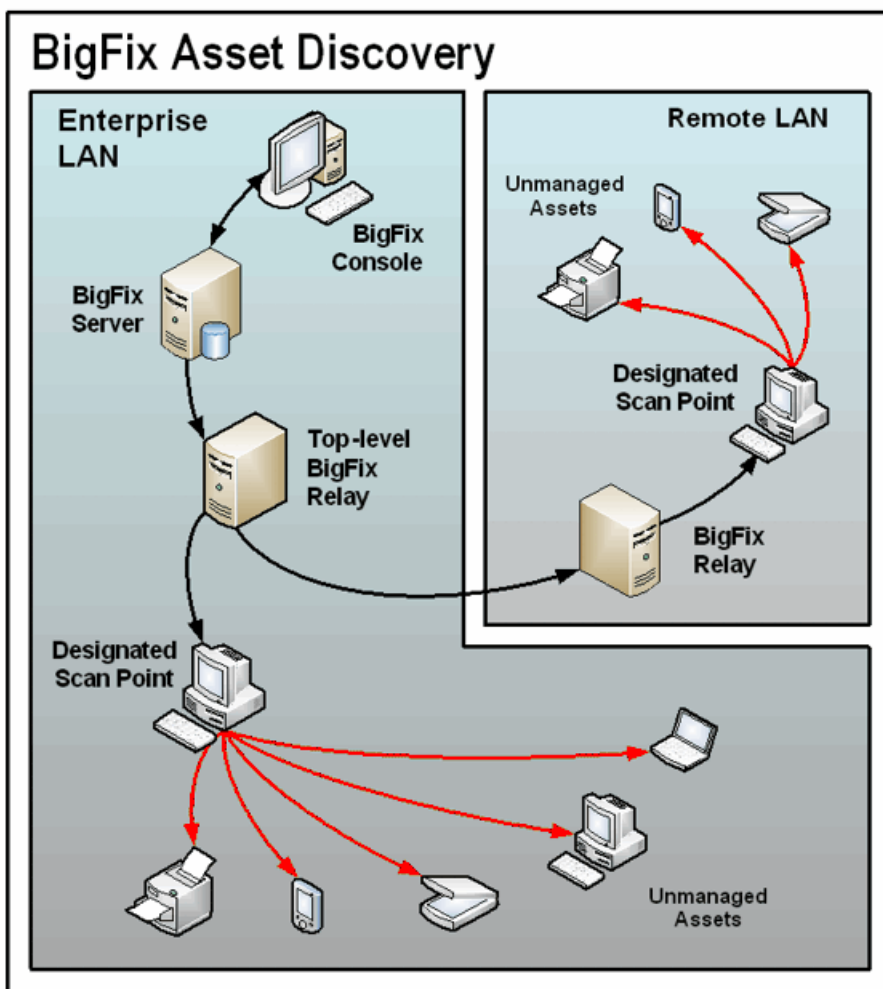
**BigFix プラットフォーム  
Asset Discovery ユーザーズ・ガイド**



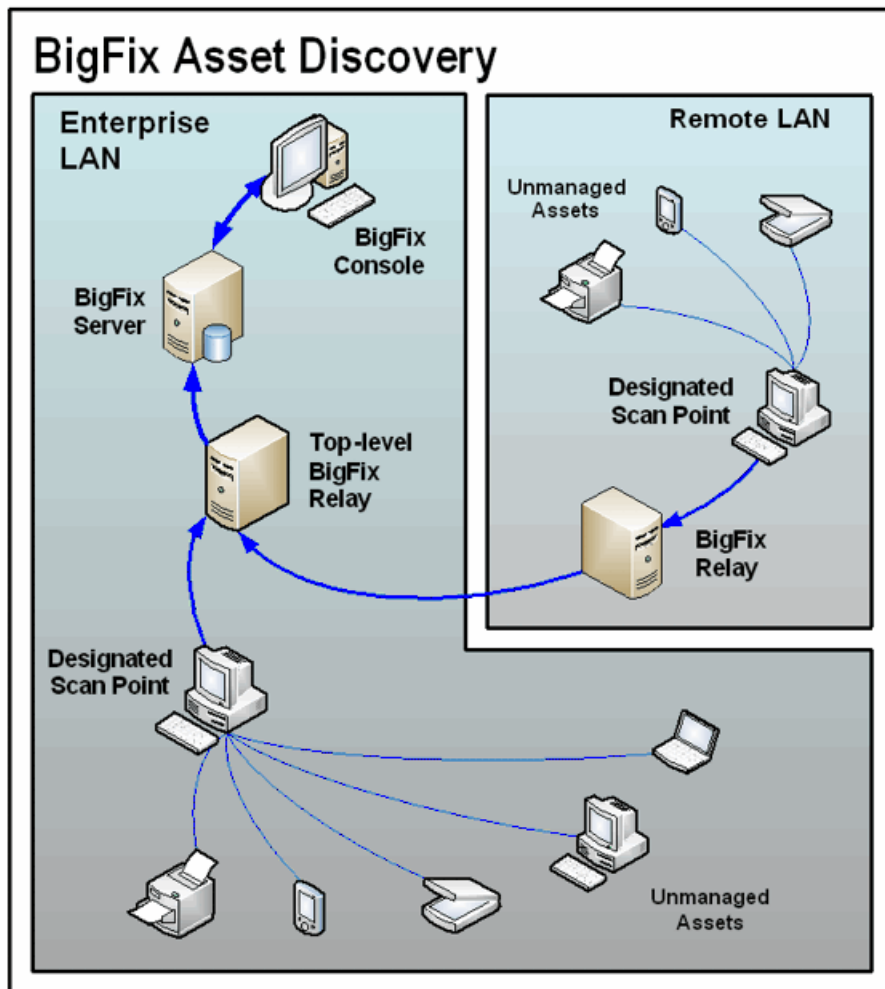
# 第 1 章 概要

BigFix が資産を発見する方法と、スキャン・ポイントについての概要を説明します。

BigFix Asset Discovery は、特定のコンピューターをスキャン・ポイントとして指定することで動作します。サポートされるオペレーティング・システムを実行しているエージェントであれば、どのエージェントもスキャン・ポイントとして指定できます。これらのスキャン・ポイントは、ネットワーク内の非管理資産を照会します。次の図は、このプロセスを示したものです。



情報は、スキャン・ポイントによってこれらの非管理資産から取得され、リレーを介して、BigFix サーバー上のデータベースに送り返されます。以下のように、このデータベースから、BigFix コンソールで結果を調べることができます。



## システム要件

スキャン・ポイント・ハードウェア要件およびソフトウェア要件

BigFix Asset Discovery では、Windows 7、Windows Vista、Windows 2008、Windows 2012、Windows 2016、Windows 2019、Windows 8、Windows 10 または Red Hat Enterprise Linux 6、および Red Hat Enterprise Linux 7、x86-64 アーキテクチャーがサポートされます。さらに、Nmap の旧バージョンでは、BigFix Asset Discovery は Red Hat Linux 5、CentOS 5、および Linux Tiny Core 8.2. もサポートします。


nmap.org Web サイトによると、Nmap では、Windows 7 以降、および Windows Server 2008 以降がサポートされます。また、Nmap は Linux オペレーティング・システムもサポートします。


## インストール

正常なインストールを完了するために実行するタスクについて説明します。

Asset Discovery サイトで、以下のインストール・タスクを実行します。

- お使いの BigFix サーバーで、Unmanaged Asset Importer サービスを有効にします。
- 特定のエージェントをスキャン・ポイントとして指定します。
- スキャンを実行します。

 **注:** 「非管理資産」を表示するには、管理ツールを通してユーザーに適切な権限が設定されていなければなりません。このツールにアクセスするには、「**スタート**」 > 「**すべてのプログラム**」 > 「**BigFix Enterprise**」 > 「**BES 管理ツール**」をクリックします。ユーザーには、すべての非管理資産を表示する許可を付与することも、管理するスキャン・ポイントに接続されている非管理資産のみ表示する許可を付与することもできます。

 **注:** Linux プラットフォームで Asset Discovery Fixlet を使用するには、BES サーバー・プラグイン・サービスをインストールする必要があります。このプラグインは、BigFix サポート・サイトで入手できます。

## サイトのインストール

すべてのコンピューターを外部サイトに対して有効にし、サブスクライブするための手順について説明します。

BigFix コンソールを使用して、外部サイトを有効にし、すべてのコンピューターを外部サイトにサブスクライブするには、次の手順を実行します。

1. 「BigFix 管理」ドメインを開き、上部までスクロールして関連付けられたダッシュボードを表示します。

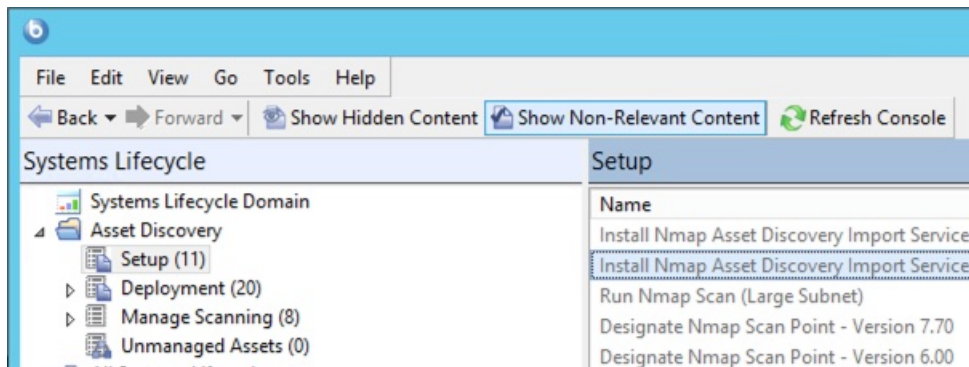
2. ライセンス・ダッシュボードで、外部サイトをクリックし、まだ外部サイトが有効になっていない場合は、サイトのリストでサイトの名前をクリックして有効にします。
3. 外部サイトのプロパティ・パネルで、「**コンピューターのサブスクリプション**」タブを選択し、「**すべてのコンピューター**」をクリックして BigFix 環境内のすべてのコンピューターを外部サイトにサブスクライブします。
4. 「**変更を保存**」をクリックして、サイト・サブスクリプション設定を保存します。

## インポート・サービス・タスクのインストール

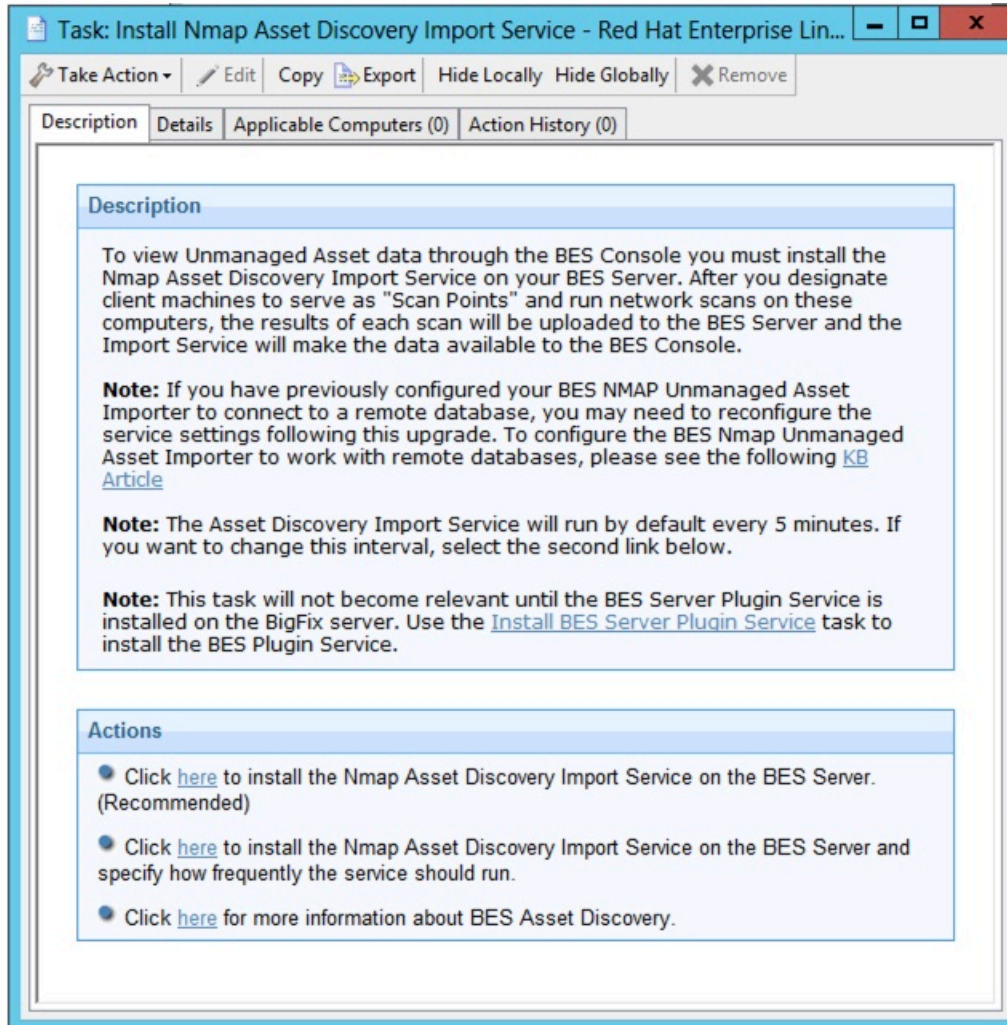
Nmap Asset Discovery インポート・サービスを BigFix サーバーにインストールする方法について説明します。

**注:** リモート・データベースにアクセスする場合は、NMAP インポート・サービスをドメイン・ユーザーとして実行する必要があります。これは、SQL データベースへのアクセスには標準ローカル・システムを使用することができないからです。このサービスは、リモート・データベース環境内の他の BigFix サービスと同様に構成する必要があります。

Asset Discovery ナビゲーション・ツリーの「設定」ノードを選択して、右側のパネルに「Nmap Asset Discovery インポート・サービスのインストール」タスクを見つけます。



このタスクをクリックし、ワークエリアで説明を確認します。

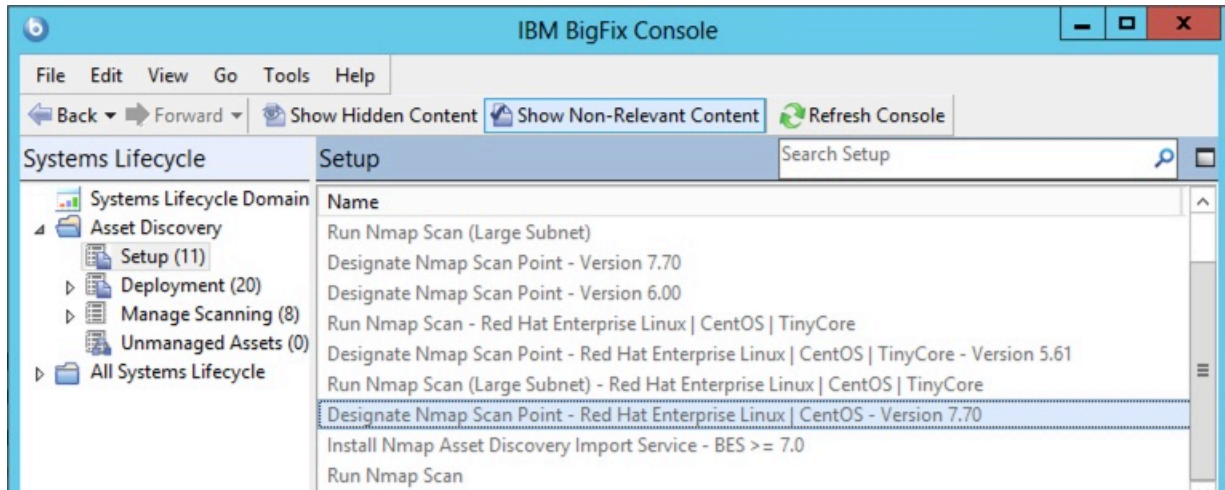


Nmap Asset Discovery インポート・サービスを BigFix サーバーにインストールするには、「アクション」ボックス内の該当するリンクをクリックします。インポート・サービスはデフォルトでは 5 分おきに実行され、BigFix サーバーに送信された新しい Nmap スキャン・データがないかどうか調べられます。別の頻度を設定する場合は、2 番目のアクション・リンクを選択します。

## スキャン・ポイントのインストール

スキャン・ポイントをインストールするためのアクションについて説明します。

Asset Discovery ナビゲーション・ツリーの「設定」ノードを選択して、右側のパネルに指定タスクを見つけます。



スキャン・ポイントとして指定するコンピューターは、Windows または Linux を実行していない必要があります。これらのスキャン・ポイントは、ローカル・サブネットをスキャンする起点となるハブです。

Info-zip の使用許諾契約を確認することもできます。

Windows の場合、「Nmap スキャン・ポイントの指定」タスクをクリックします。

「アクション」ボックスの最初のリンクをクリックして、「アクションの実行」ダイアログにアクセスします。「対象」タブから、スキャン・ポイントとして指定するコンピューターを選択します。

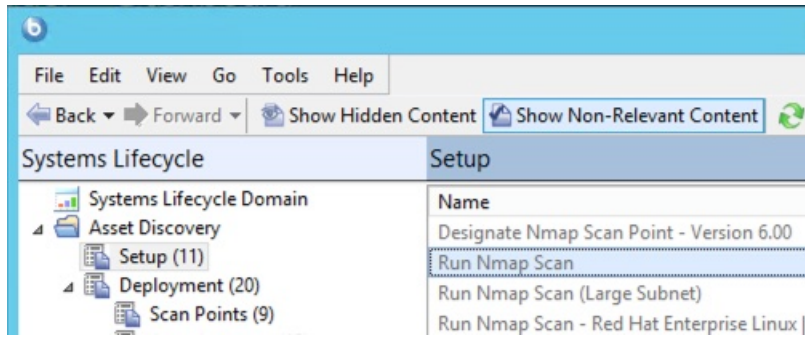
Linux の場合、「Nmap スキャン・ポイントの指定 - Red Hat Enterprise Linux」タスクをクリックします。

「アクション」ボックスの最初のリンクをクリックして、Nmap スキャン・ポイントを指定します。

## スキャンの実行

非管理コンピューターと非管理ネットワーク・デバイスを検出するためのスキャンを実行する方法について説明します。

Asset Discovery ナビゲーション・ツリーの「設定」ノードを選択して、「Run Nmap Scan」で使用可能なすべてのタスクを見つけます。



ワークエリアでこのタスクが開いたら、「アクション」ボックスで、Nmap スキャンを開始するための有効なリンクの 1 つを選択します。ローカル・サブネットまたは大規模サブネットを指定できます。



**Task: Run Nmap Scan - IBM BigFix Console**

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

**Description**

This task will run an Nmap scan from the selected computers to detect unmanaged computers and network devices. Use the links below to either scan the entire local subnet or to specify a particular IP range.

Once complete, the scan data will be uploaded to the BES Server and automatically imported into the BES Server database by the Asset Discovery Import Service. You will then be able to view the results through the Unmanaged Assets report interface.

To schedule repeated scans or to specify advanced configuration options such as additional ports, timing/aggressiveness options, specific hosts to exclude, and other Nmap command line switches, use the BigFix Asset Discovery Nmap Configuration Wizard to generate a custom Nmap Scan Fixlet message.

**Important Note:** This task will remove client settings that were created by Nmap scans. By removing excessive old client settings, it will improve performance with the BES Client. By default, it will remove scans that were initiated over 7 days ago. To change this setting, run the task "Set Scanpoint Cleanup Configuration" (ID 34).

**Note:** The Nmap security scanner is used within BigFix under license from Insecure.Com LLC (The Nmap Project). For more information on Nmap, as well as advanced configuration options, visit the link below.

**Note:** Nmap supports CIDR-style addressing. For more details about how to specify an IP range, visit the link below.

**Note:** Client machines may briefly display dos and command prompt windows as a result of running the action below.

**Actions**

- Click [here](#) to run an Nmap scan on the local subnet.
- Click [here](#) to run an Nmap scan on a specific IP range.
- Click [here](#) to run Nmap on the last subnet scanned. This action is only valid if you have previously run an Nmap scan on the selected Scan Point(s).
- Click [here](#) for more information about Nmap.
- Click [here](#) for more information about BES Asset Discovery.

クラス C ネットワーク (255 個の IP アドレス) のスキャンは通常は、ご使用のネットワークに応じて、10 分から 30 分ほどかかります。Asset Discovery Nmap 設定ウィザードを使用して、Nmap スキャンをスケジュールおよび構成するための独自のカスタム・タスクを作成することもできます。

スキャン・ポイントでそのローカル・スキャンが完了すると、その結果は BigFix サーバーにアップロードされ、Importer サービスによってデータベースにインポートされます。これにより、スキャン結果が BigFix コンソールの「非管理資産」タブに表示されます。

これで、Asset Discovery サービスのインストールは完了です。

## 第 2 章. Asset Discovery の使用

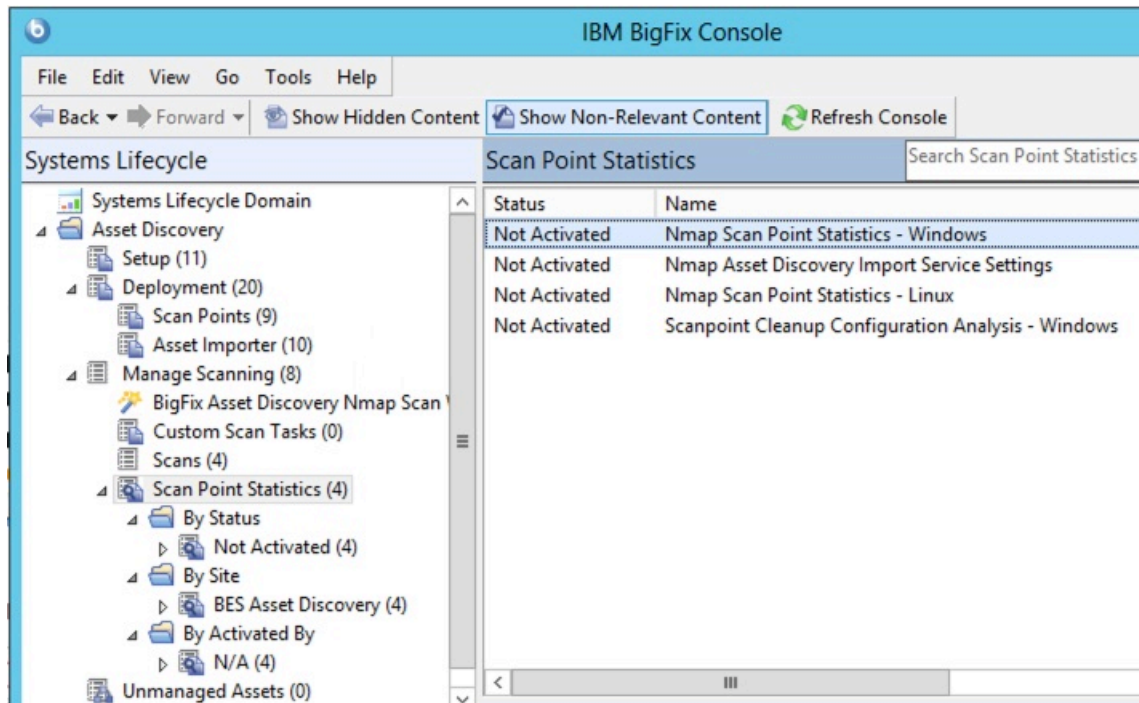
Asset Discovery の使用方法と注意事項について

### 演算

スキャン・ポイント・コンピューターが取得した非管理資産に対して実行可能なアクションについて説明します。

インストールが完了すると、スキャン・ポイント・コンピューターによって取得されたすべての非管理資産情報を表示できます。

任意の時点で、「スキャン・ポイント統計」をアクティブにして、指定された Nmap スキャン・ポイントに関する情報を表示することができます。ナビゲーション・ツリーの「スキャンを管理」ノードの下にある「スキャン・ポイント統計」をクリックします。統計は、「ステータス別」、「サイト別」、または「アクティベーション別」に表示できます。



スキャン・ポイント・コンピューターを解除する場合は、「インストール」ノードの「Nmap スキャン・ポイントの削除」タスクを使用します。「Nmap スキャン・ポイン

トの削除」タスクにアクセスするには、「インストール」ノードの下の「スキャン・ポイント」をクリックします。

The screenshot shows the BigFix console interface. At the top, there is a 'Deployment' header with a search bar. Below it is a table of deployment tasks:

Name	Source	Severity	Site	Applica
Designate Nmap Scan Point - Version 7.70	<Unspecified>		BES Asset Discov...	0 / 0
<b>Remove Nmap Scan Point - Version &gt;= 7.70</b>	<Unspecified>		BES Asset Discov...	0 / 0
Designate Nmap Scan Point - Red Hat Enterprise Linux   CentOS - Version 7.70	<Unspecified>		BES Asset Discov...	0 / 0
Upgrade Nmap - Version 6.00			BES Asset Discov...	0 / 0
Change UAlmporter Delete Mode			BES Asset Discov...	0 / 0

Below the table, the selected task 'Task: Remove Nmap Scan Point - Version >= 7.70' is expanded. It features a toolbar with 'Take Action', 'Edit', 'Copy', 'Export', 'Hide Locally', 'Hide Globally', and 'Remove'. Below the toolbar are tabs for 'Description', 'Details', 'Applicable Computers (0)', and 'Action History (0)'. The 'Description' tab is active, showing the following text:

**Description**

This task will remove previously installed Nmap components and configuration settings from targeted machines. After deploying this Task, these computers can no longer be used to scan your network.

**Note:** The actions below will also remove all run statistics for Nmap from selected computers.

**Actions**

- Click [here](#) to uninstall Nmap and Npcap.
- Click [here](#) to uninstall Nmap only.
- Click [here](#) for more information about Nmap.
- Click [here](#) for more information about BES Asset Discovery.

これにより、指定されたスキャン・ポイントから Nmap が削除され、Nmap の最新バージョンで WinPcap または Npcap も削除できます。「アクション」ボックスをクリックして、「アクションの実行」ダイアログにアクセスし、解除するスキャン・ポイント・コンピューターを選択します。非管理資産を削除するには、ナビゲーション・ツリーの一番下にある「非管理資産」をクリックします。

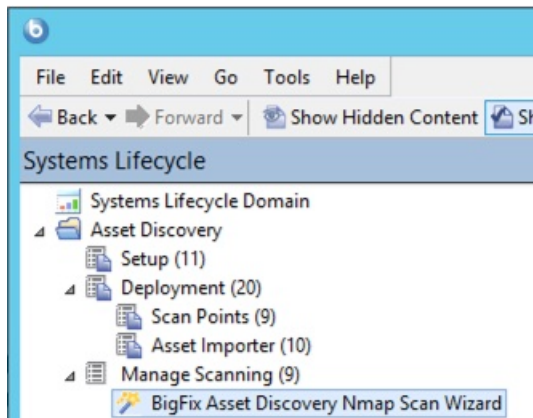
## Nmap スキャン・ウィザードの使用

Nmap スキャナーを要件に合わせてカスタマイズする方法について説明します。

Asset Discovery Nmap スキャン・ウィザードを使用すると、Nmap スキャン・プログラムのさまざまな側面を変更できます。以前に指定したスキャン・ポイントを使用して、ネットワークの定期的な Nmap スキャンをスケジュールすることができます。

**注:** Nmap スキャン・プログラムを実行するには、`UnmanagedAssetImporter -NMAP` サービスがサーバー上で実行されている必要があります。

ナビゲーション・ツリーの「スキャンを管理」ノードの下にある「スキャン・ウィザード」をクリックします。



右側にウィザードが表示されます。

BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard. Progress:

Please select one of the following options:

- Scan the local subnet.**  
This option is only valid if the local subnet of the Scan Point is a Class C subnet and it is only one.
- Scan the following hosts:**  
Separate multiple subnets or IP ranges with a single space (ex: 192.168.100.1-254 10.0.0.0/24).  
[Nmap command line options for host specification.](#)

まず、スキヤンのタイプを選択します。ローカル・サブネットをスキヤンするか、特定のホストをスキヤンすることができます。「次へ」をクリックします。

「ローカル・サブネットをスキヤンする」を選択した場合は、次の画面で、このスキヤンの固有パラメーターを設定します。ウィンドウの上部にある進行状況表示バーを確認してください。

The screenshot shows the 'Nmap Scan Options' step of the BigFix Asset Discovery Nmap Scan Wizard. The window title is 'BigFix Asset Discovery Nmap Scan Wizard'. At the top, a message states: 'This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".' Below this is a progress bar with three steps: 'Welcome to the BigFix Asset Discovery Nmap Scan Wizard.', 'Nmap Scan Options' (the current step), and 'Progress:'. The main content area contains the following options:

- Nmap Scan Options**  
For more information on what these settings mean, click [here](#).
- Enter the TCP ports you want to scan.** Separate each port or port range with a single space.  
Input field: 22 23 80 135 139 445 61616
- Select the timing policy that you want.** The higher the value, the more aggressive the scan. Note that more aggressive scans will induce a greater load to your network.  
Options:  0 - Paranoid  1 - Sneaky  2 - Polite  3 - Normal  4 - Aggressive  5 - Insane
- Run OS Detection.** Selecting "Yes" will cause Nmap to try and detect operating system information.  
Options:  Yes  No
- Enable version detection.** Selecting "Yes" will cause Nmap to detect services running on open ports.  
Options:  Yes  No
- List any hosts you want to exclude from this scan.** Delimit multiple host addresses and/or ranges with commas (ex: 192.168.100.1-5,10,15)  
Input field: (empty)

At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

この画面では、ポートのスキャン、オペレーティング・システム検出の実行、バージョン検出の有効化、および除外するホストのリストについて設定します。必要な選択を行って、「次へ」をクリックします。

次の画面では、Nmap Configuration 設定オプションの有効化、ping オプションの選択、その他の Nmap スキャン・オプションの入力ができます。必要な選択を行って、「次へ」をクリックします。

BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard. → Nmap Scan Options → Progress:

**Enable Advanced Nmap Configuration Options.** →

**Enable Advanced Nmap Configuration Options.**

**Select ping options.** By default, Nmap uses ICMP echo requests and TCP ACK pings on port 80 in parallel.

- P0: Do not try to ping hosts before scanning.
- PE: Use ICMP echo request packets to ping hosts.
- PA: Use TCP ACK packets to ping hosts. Specify destination port below.
- PS: Use TCP SYN packets to ping hosts. Specify destination port below.

**Enter additional Nmap scan options.** Separate each option with a space. These switches will be appended to the command line call to Nmap. [Nmap command line reference guide.](#)


Take this action immediately.

次の画面では、Fixlet のテキスト・フィールドをカスタマイズできます。Fixlet のタイトルと説明を編集できます。すべてのテキスト・フィールドをカスタマイズしたら、「完了」をクリックして、プライベート・キーのパスワードを入力します。



BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard. → Nmap Scan Options → Progress: 

Enable Advanced Nmap Configuration Options. → Customize the text fields for this Fixlet message.

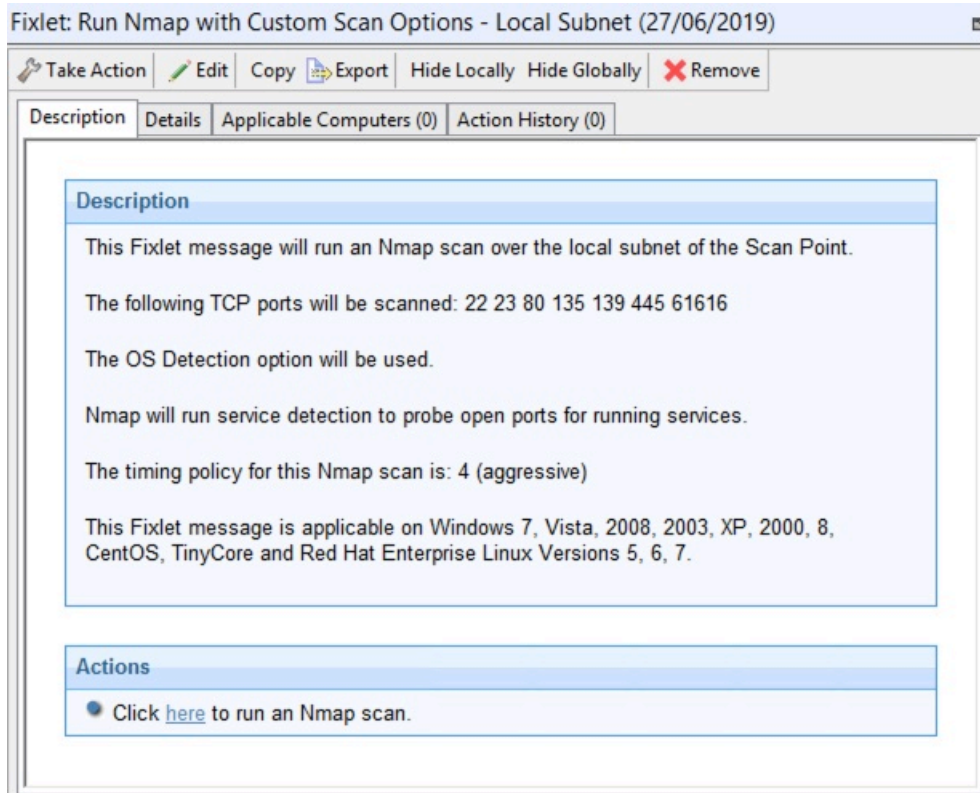
**Note:** If you choose to edit this page, the default title and messages will not be regenerated by the Wizard, even in the event you go back and modify previous input.

**Edit the title:**

**Edit the description:**  
  
The following TCP ports will be scanned: 22 23 80 135 139 445 61616  
The OS Detection option will be used.  
Nmap will run service detection to probe open ports for running services.

Show Custom Fixlet Dialog before creating this Fixlet message.

これにより、ウィザードで入力した固有のパラメーターおよびカスタマイズが含まれる Fixlet が表示されます。「説明」フィールドのテキストを確認し、「アクション」ボックス内の該当するリンクをクリックして、Nmap スキャンを実行します。



## 考慮事項

ライセンスとスキャンに関する潜在的な問題についての注意事項。

### ライセンス


- スキャン・ポイントを指定するときは、Nmap と Npcapをインストールします。Nmap セキュリティー・スキャナーおよび Npcap パケット・キャプチャー・ライブラリーは Insecure.Com LLC のライセンスの下で BigFix 内で使用されています (The Nmap Project)。
- Nmap は .zip ファイルとして配布されます。このファイルを解凍するために、BigFix は一時的に Info-Zip の解凍ツールをダウンロードして使用します。Info-Zip は、オープン・ソース解凍ユーティリティーです。Info-Zip について詳しくは、<http://www.info-zip.org/> を参照してください。

### スキャンに関する潜在的な問題

- ネットワーク・スキャンを実行すると、侵入検知システムが起動する可能性があります。この可能性を最小限に抑えるには、Nmap スキャン・モードを 0 (「Paranoid」) に設定するか、Nmap スキャンが許可されるように IDS を変更します。これにより、スキャンにかかる時間が長くなる場合があります。
- 一部のレガシー・ネットワーク・デバイス (古いネットワーク・プリンター・デバイスなど) では、ネットワーク・スキャンの実行が原因となってエラーが発生することがあります。
- ネットワーク・スキャンを実行すると、個人用ファイアウォールから、コンピューターがローカル・コンピューターをスキャンしていると通知される場合があります。Nmap スキャンを許可するように、ご使用のファイアウォールを変更してください。
- Nmap は、ウィルス・スキャン・プログラムによって、有害の恐れがあるツールとしてフラグが立てられる場合があります。ウィルス・スキャン・プログラムは、Nmap の実行を妨げないように設定してください。
- 大規模ネットワークをスキャンするように Nmap を設定した場合は、処理に数時間かかり、スキャン中にかなりの帯域幅を使用する可能性があります。デフォルトのスキャンはローカルのクラス C ネットワークであり、これは通常は高速 LAN です。WAN にまたがる大規模ネットワークをこのツールでスキャンすることはお勧めしません。
- Nmap を使用したスキャンは一般的にはいたって安全な操作ですが、対処が必要な組織固有の問題が存在する場合があります。作業に進む前に、ネットワーク・チームから適切な許可を得てください。
- スキャン・ポイント名に非 ASCII 文字を含めることはできません。マスター以外のオペレーターが「スキャン・ポイント別」を実行するか、または BigFix サーバーへのスキャン・レポートのアップロードに失敗する場合、非 ASCII 文字があると、非管理資産が見つからなくなる可能性があります。

## 第 3 章. Unmanaged Asset Importer - NMAP

インポーターを単体で実行するには、以下のオプションがコマンドライン引数として動作します。例えば、「UAImporter-NMAP -debugout output.txt -file testfile.xml」です。

 **注:** 同じ引数がクライアント設定としてまだ定義されていない場合のみ、コマンド行で指定された引数が考慮されます。それ以外の場合は、クライアント設定が使用されます。

### Windows BigFix サーバー

これらのオプションは `HKLM\Software\BigFix\Enterprise Server\AssetDiscover\NMAP` の下にあります。

- "DSN"[REG\_SZ]

リモート・データベースに使用される DSN。デフォルトは `bes_bfenterprise` です。

- "username"[REG\_SZ]

SQL のユーザー名。デフォルト設定は NT 認証です。

- "password"[REG\_SZ]

SQL のパスワード。デフォルトは NT 認証です。

- "file"[REG\_SZ]

このファイルをデータベースにインポートするだけです。ファイルの形式は、「`nmap-NameOfYourChoice-1570442924`」の形式にする必要があります。ここでは、「`nmap`」が接頭部で、「`1570442924`」がタイム・スタンプです。その間に任意の名前を入れます。

- "filedirectory"[REG\_SZ]

このディレクトリー内のすべてのファイルをデータベースにインポートするだけです。

- "port"[REG\_SZ]

BigFix クライアントを実行しながら、資産をフィルタリングによって除外する際に使用する BigFix ポート番号

- "filteroutclients"[REG\_SZ]

BigFix クライアントをフィルタリングで除去するには 1 に設定、BigFix クライアントを含めるには 0 に設定します。デフォルトは 1 です。

- "serviceinterval"[REG\_SZ]

資産のバッチのインポートを試行中にサービスがスリープすべき秒数。デフォルトは 300 です。

- "osfamilyclientexemptions"[REG\_SZ]

os ファミリーのストリング。nmap によって、資産にこれらのファミリーの 1 つが含まれていると報告される場合、クライアントがないと見なされます。これは、デバイスがポート 52311 を listen しているため、クライアントがインストールされているとインポーターが見なす場合に役立ちます。しかし、クライアントがないのはプリンターやその他のデバイス・タイプであるため、クライアントが実行されていないことは明確です。デフォルトは「embedded;IOS;DYNIX」です。

- "usegmt"[REG\_SZ]

「スキャン時刻」と「インポート時刻」をサーバーの時刻にするは 0 に設定、GMT にするには 1 に設定します。デフォルトは 0 です。

- "showevenifexactmatch"[REG\_SZ]

1 に設定すると、BigFix コンピューターが一致する (MAC アドレス、IP アドレス、ホスト名に基づく) 資産を含めます。デフォルトは 0 です。

- "debugout"[REG\_SZ]

このキーがファイルを指す場合、UnmanagedAssetImporter-NMAP はそのファイルにデバッグ出力を印刷します。デバッグ出力へのデフォルト・パスは "" です。

- "filteroutdownhosts"[REG\_SZ]

1 に設定すると、状態が「ダウン」の資産をインポートしません。デフォルトは 1 です。

- "ignoredeletedassets"[REG\_SZ]

1 の場合、削除された資産は無視され、以降のスキャンにおいて戻されません。0 の場合、削除された資産は再スキャンにおいて復元されます。デフォルトは 1 です。

## Linux BigFix サーバー

これらのオプションは、besclient.config ファイルにあります。オプションの定義については、上記のセクションを参照してください。

- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_debugout]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_file]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_filedirectory]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_port]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_filteroutclients]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_serviceinterval]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_osfamilyclientexemptions]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_usgmt]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_showevenifexactmatch]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_filteroutdownhosts]
- [Software\BigFix\EnterpriseClient\Settings\Client\\_AssetDiscovery\_ignoreddeletedassets]

## 第 4 章 よくある質問

よくある質問のリスト。

### 「非管理資産」はどのように識別されますか？

2 つの「非管理資産」で、MAC アドレスが既知の場合、MAC が同じであれば一致となりますが、それ以外は一一致となりません。2 つの「非管理資産」で、MAC アドレスの 1 つが既知のものでなく、ホスト名が既知の場合、ホスト名が同じであれば一致となりますが、それ以外は一一致となりません。両方の「非管理資産」に MAC アドレスもホスト名も無い場合、IP アドレスが同じであれば一致となりますが、それ以外は一一致となりません。

### スキャンを開始しましたが、結果はどこにありますか。

Asset Discovery を初めてインストールした場合は、最初にシステムをスキャンして非管理資産について報告するのに、数分かかる可能性があります。20 分経過しても BigFix コンソールに何も表示されない場合は、キーボードの F5 を押して、強制的にフル・リフレッシュを実行してください。

### 「非管理資産」タブは、どこに表示されるのですか。

「非管理資産」タブは、Nmap Asset Discovery インポート・サービスをインストールして初めて表示されます。インターフェースに表示されるのに数分かかる可能性があります。このタブが表示されたら、タブを開き、個々の資産をクリックして、その資産の詳細を確認することができます。

### 標準的なスキャンにはどのくらいの時間がかかりますか。

クラス C サブネットをスキャンすると、通常は 10 分から 30 分かかりますが、これは、ご使用のネットワークによって変わる可能性があります。より大規模なネットワークでは、スキャンの実行に数時間かかる場合があります。

### 帯域幅の要件はどのようになっていますか。

Nmap スキャン・プログラムは、帯域幅の問題を引き起こす可能性の低い、小さいパケットを送信します。これは、このプログラムが、高速ネットワーク上で近くにあるコンピューターをスキャンするように設計されていることが主な理由です。スキャンが完了すると、スキャン結果は BigFix サーバーにアップロードされます。通常、このファイルは比較的小さいファイルであり（一般に 10 KB から 200 KB）、スキャンされるエンドポイントの

数によって異なります。1つのスキャン・ポイントで大規模ネットワークをスキャンすると、ファイルのサイズは大きくなるがありますが、このようなスキャンは定期的にしかな行されません。

**どのくらいの頻度でスキャンを実行できますか。**

Asset Discovery が正しくセットアップされている場合、ネットワークへの影響はほとんどないため、スキャンをかなり頻繁に実行しても、問題はありません。無許可のネットワーク・デバイスを検出するために、スキャンを1日に何度も実行してもかまいません。あるいは、正確なネットワーク・インベントリ情報を維持するために、頻度を低くすることもできます。

**Nmap スキャン設定は変更できますか。**

はい。デフォルトの Nmap スキャン設定は、高速で完全なスキャンを可能にします。この設定は、必要に応じて Nmap 設定ウィザードで変更することができます。これにより、すべての可能な Nmap 設定に対応できます。